Золотая середина. Обзор инструментов для проведения MITM-атак

Антон Жуков , 26.06.2015 Комментарии 79,249 Добавить в закладки



Содержание статьи

01. MITMf
02. PuttyRider
03. sessionthief
04. ProxyFuzz
05. The Middler
06. Mitmproxy
07. Intercepter-NG
08. Subterfuge
09. Dsniff
10. KARMA
11. AirJack
12. SSLsplit
13. Ettercap
14. In The End

Добиваться желаемого результата почти всегда можно несколькими способами. Это применимо и к области ИБ. Иногда для достижения цели можно брутить, самостоятельно искать дыры и разрабатывать сплоиты или же прислушаться к тому, что передается по сети. Причем последний вариант зачастую бывает оптимальным. Именно поэтому сегодня мы поговорим об инструментах, которые помогут вылавливать ценную для нас информацию из сетевого трафика, привлекая для этого MITM-атаки.

MITMf

Ссылка на сайт

Начнем с одного из наиболее интересных кандидатов. Это целый фреймворк для проведения man-in-the-middle атак, построенный на базе sergio-proxy. С недавнего времени включен в состав Kali Linux. Для самостоятельной установки достаточно клонировать репозиторий и выполнить пару команд:

```
# setup.sh
# pip install -r requirements.txt
```

Имеет расширяемую за счет плагинов архитектуру. Среди основных можно выделить следующие:

- Spoof — позволяет перенаправлять трафик при помощи ARP/DHCP-спуфинга, ICMP-редиректов и модифицировать DNS-запросы;
- Sniffer — этот плагин отслеживает попытки логина для различных протоколов;
- BeEFAutorun — позволяет автоматически запускать модули BeEF, исходя из типа ОС и браузера клиента;
- AppCachePoison — осуществляет атаку «отравление кеша»;
- SessionHijacking — угоняет сессии и сохраняет полученные куки в профиле огнелиса;
- BrowserProfiler — пытается получить список используемых браузером плагинов;
- FilePwn — позволяет подменять пересылаемые по HTTP файлы с помощью Backdoor Factory и BDFProxy;
- Inject — внедряет произвольный контент в HTML-страницу;
- jskeylogger — внедряет JavaScript-кейлоггер в клиентские страницы.

Если данного функционала тебе покажется недостаточно, то ты всегда можешь добавить свой, реализовав соответствующее расширение.

```
byt3bl33d3r@holeechit:~/MITMf$ sudo python mitmf.py --arpspoof --iface wlan0 --routerip 192.168.10.1 --target 192.168.10.5
[sudo] password for byt3bl33d3r:
[*] MITMf v0.1 started... initializing plugins and modules
[*] ARP Spoof plugin online
[*] Setting up ip_forward and iptables

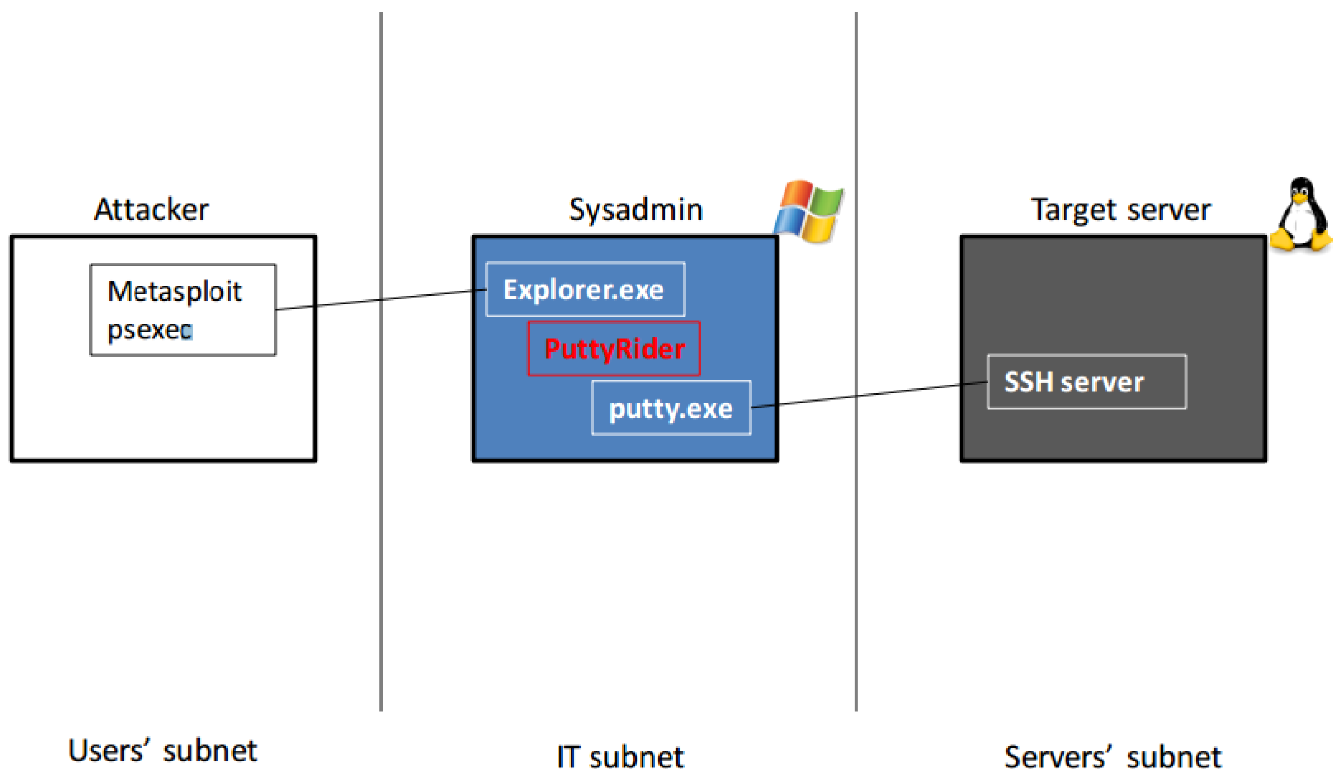
[*] sslstrip v0.9 by Moxie Marlinspike running...
[*] sergio-proxy v0.2.1 online
```

Запуск ARP spoofing атаки в MITMf

PuttyRider

Ссылка на сайт

Еще одна достойная внимания утилита. Правда, в отличие от всех остальных рассматриваемых сегодня инструментов, она очень узко специализирована. Как рассказывает сам автор проекта, на мысль создать такую утилиту его натолкнуло то, что во время проведения тестов на проникновение наиболее важные данные располагались на Linux/UNIX-серверах, к которым админы подключались по SSH/Telnet/rlogin. Причем в большинстве случаев получить доступ к машине администраторов было намного проще, чем к целевому серверу. Проникнув на машину сисадмина, остается только убедиться в наличии запущенного PuTTY и с помощью данной тулзы выстроить обратный мостик до атакующего.



Принцип работы PuttyRider

Утилита позволяет не только снифать «общение» между админом и удаленным сервером (включая пароли), но и выполнять произвольные shell-команды в рамках данной сессии. Причем все это будет происходить абсолютно прозрачно для пользователя (админа). Если интересуют технические детали, например как реализовано внедрение в процесс PuTTY, рекомендую ознакомиться с презентацией автора.

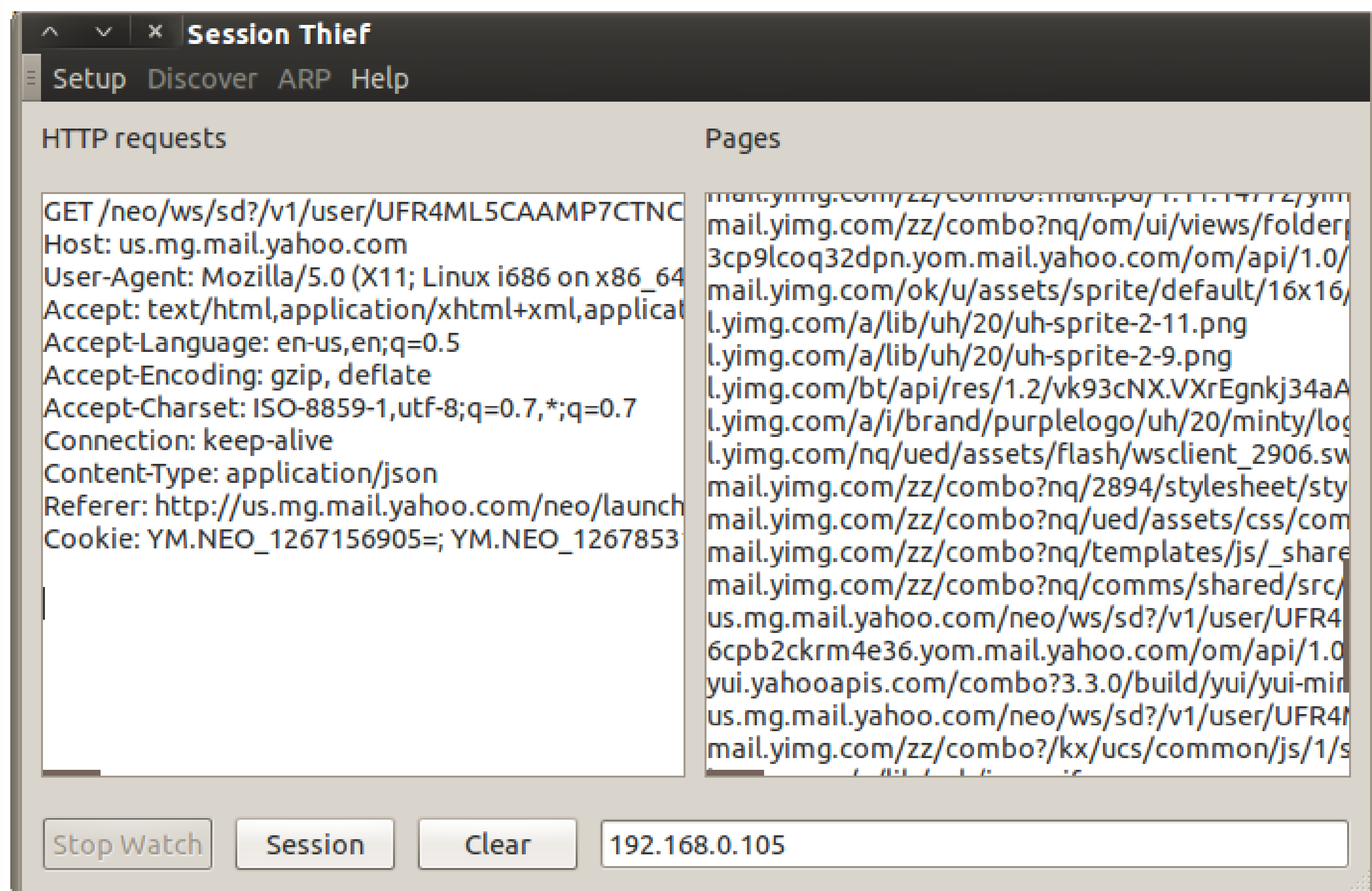
Архитектура PuttyRider

sessionthief

Ссылка на сайт

Довольно старая утилита, появившаяся на свет более восьми лет назад. Предназначается для клонирования сессий путем кражи кукисов. Для угона сессий имеет базовые навыки обнаружения хостов (в случае подключения к открытой беспроводной сети или хабу) и проведения ARP poisoning. Единственная проблема — сегодня, в отличие от того, что было восемь лет назад, почти все крупные компании, такие как Yahoo или Facebook, используют SSL-шифрование, что делает эту тулзу абсолютно бесполезной. Несмотря на это, в Сети еще остается достаточно ресурсов, не использующих SSL, так что списывать утилиту со счетов пока рано. К ее плюсам можно отнести то, что она автоматически интегрируется в Firefox и создает отдельный профиль для каждой перехваченной сессии. Исходный код доступен в репозитории, а самостоятельно собрать ее можно с помощью такой последовательности команд:

```
# apt-get install build-essential libwxgtk2.8-dev libgtk2.0-dev libpcap-dev
# g++ $(wx-config --cppflags --libs) -lpcap -o sessionthief *.cpp
# setcap cap_net_raw,cap_net_admin=eip sessionthief
```



Sessionthief

ProxyFuzz

Ссылка на сайт

Непосредственно к проведению MITM-атак ProzyFuzz не имеет никакого отношения. Как можно догадаться из названия, тулза предназначена для фаззинга. Это маленький недетерминированный сетевой фаззер, реализованный на питоне, который произвольно меняет содержимое пакетов сетевого трафика. Поддерживает протоколы TCP и UDP. Можно настроить, чтобы производился фаззинг только одной стороны. Пригодится, когда нужно быстренько проверить какое-нибудь сетевое приложение (или протокол) и разработать PoC. Пример использования:

```
python proxyfuzz -l <localport> -r <remotehost> -p <remoteport> [options]
```

Список опций включает в себя:

- w — задает число запросов, отправленных перед началом фаззинга;
- c — фаззить только клиента (иначе обе стороны);

- s — фаззить только сервер (иначе обе стороны);
- u — UDP-протокол (в противном случае используется TCP).

The Middler

Ссылка на сайт

Представленная в рамках конференции DEF CON утилита для проведения MITM-атак на различные протоколы. Альфа-версия поддерживала протокол HTTP и имела в своем арсенале три крутых плагина:

- plugin-beef.py — внедряет Browser Exploitation Framework (BeEF) в любой HTTP-запрос, приходящий из локальной сети;
- plugin-metasploit.py — внедряет в незашифрованные (HTTP) запросы IFRAME, который подгружает эксплойты для браузеров из Metasploit;
- plugin-keylogger.py — встраивает JavaScript обработчик события onKeyPress для всех текстовых полей, которые будут передаваться по HTTPS, заставляя браузер посимвольно отправлять вводимый пользователем пароль на сервер атакующего, до того как произойдет отправка всей формы.

The Middler не только автоматически анализирует сетевой трафик и находит в нем кукисы, но и самостоятельно запрашивает их со стороны клиента, то есть процесс автоматизирован по максимуму. Программа гарантирует сбор всех незащищенных аккаунтов в компьютерной сети (или публичном хотспоте), к трафику которой она имеет доступ. Для корректной работы программы в системе должны быть установлены следующие пакеты: Scapy, libpcap, readline, libdnet, python-netfilter. К сожалению, репозиторий давно не обновляется, поэтому новую функциональность придется добавлять самостоятельно.

Mitmproxy

Ссылка на сайт

Консольная утилита, которая в интерактивном режиме позволяет исследовать и модифицировать HTTP-трафик. Благодаря таким навыкам утилита используется не только пентестерами/хакерами, но и обычными разработчиками, применяющими ее, например, для отладки веб-приложений. С ее помощью можно получать подробную информацию о том, какие запросы делает приложение и какие ответы оно получает. Также mitmproxy может помочь в изучении особенностей функционирования некоторых REST API, в особенности плохо документированных.

Установка предельно проста:

```
$ sudo aptitude install mitmproxy
```

или

```
$ pip install mitmproxy
```

или же

```
$ easy_install mitmproxy
```

Стоит отметить, что mitmproxy позволяет также выполнять перехват HTTPS-трафика, выдавая клиенту самоподписанный сертификат. Хороший пример того, как настроить перехват и модификацию трафика, можно посмотреть по этой ссылке.

```
~/git/public/mitmproxy (Python)
    GET https://github.com/
        ← 200 text/html 5.52kB
    GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github2-24f59e3ded11f2a
        1c7ef9ee730882bd8d550cfb8.css
        ← 200 text/css 28.27kB
    GET https://a248.e.akamai.net/assets.github.com/images/modules/header/logov7@4x-hover.png?1
        324325424
        ← 200 image/png 6.01kB
    GET https://a248.e.akamai.net/assets.github.com/javascripts/bundles/jquery-b2ca07cb3c906cec
        cfd58811b430b8bc25245926.js
        ← 200 application/x-javascript 32.59kB
  ↺ GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github-cb564c47c51a14
        af1ae265d7ebab59c4e78b92cb.css
        ← 200 text/css 37.09kB
    GET https://a248.e.akamai.net/assets.github.com/images/modules/home/logos/facebook.png?1324
        526958
        ← 200 image/png 5.55kB
>>  GET https://github.com/twitter

[7]    [i:.*]                                                              ?:help [*:8080]
```

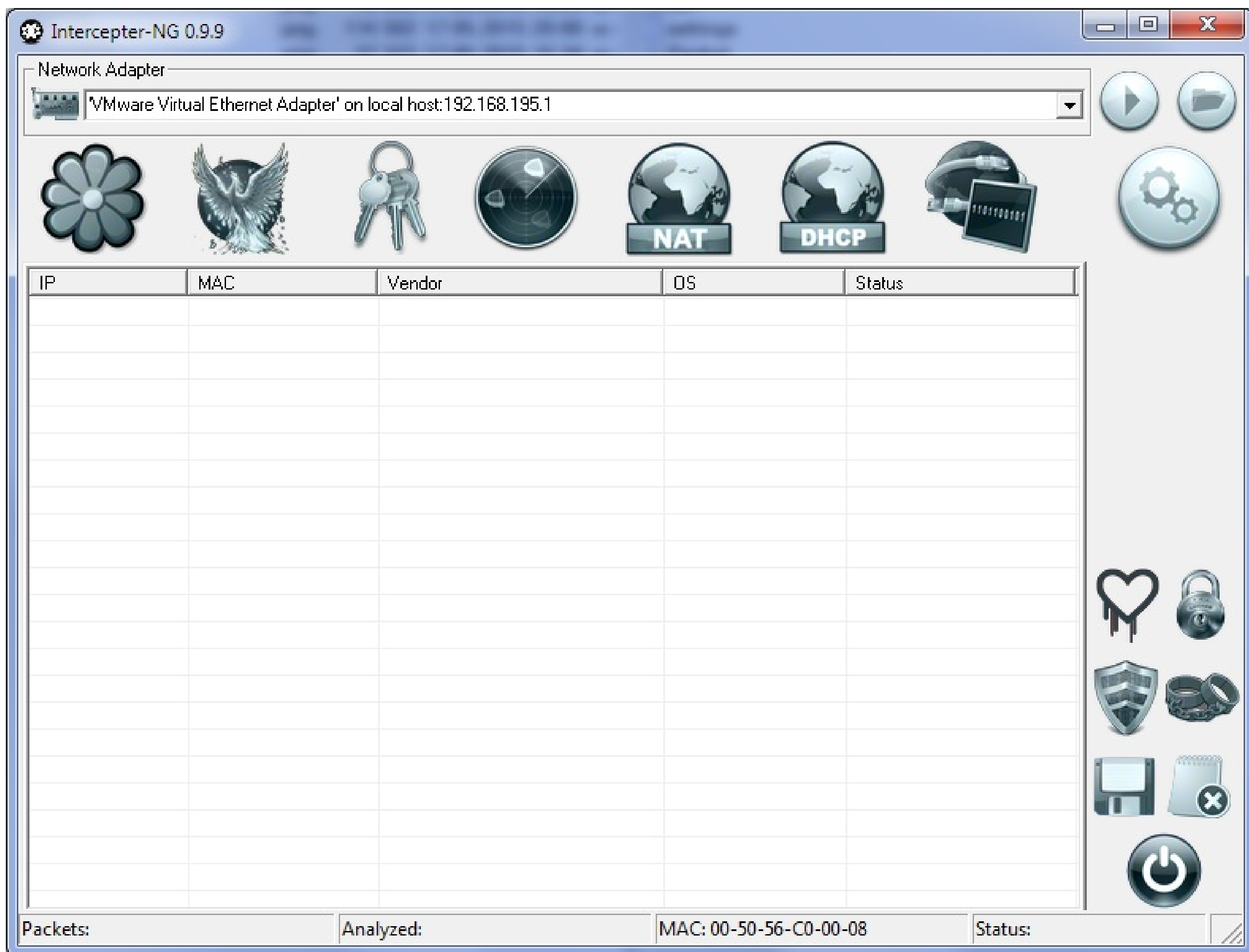
Mitmproxy

Intercepter-NG

Ссылка на сайт

Было бы странно, если бы этот легендарный инструмент не вошел в наш обзор. Даже если ты никогда его не юзал, то наверняка про него слышал (и просто обязан познакомиться с ним поближе) — он довольно часто встречается на страницах журнала. Полностью описывать его функционал не буду — во-первых, нас интересует именно MITM, во-вторых, такое описание займет всю статью.

Инструмент как нельзя лучше подходит для нашей задачи. Во-первых, он реализует множество техник для того, чтобы «устроиться посередине». Во-вторых, обладает графическим интерфейсом, правда под винду, пользователям nix-систем придется довольствоваться консольной версией (но, как говорит автор, последнюю версию можно запустить под Wine и наслаждаться тем же GUI). Ну а теперь поподробней про MITM. Вариантов тут действительно хватает. Есть классический ARP poison. Затем спуфинг (поддерживаются протоколы DNS/NBNS/LLMNR). DNS over ICMP Redirect, пришедшая на смену простому ICMP Redirect'у. DHCP MITM, SSL MITM + SSLStrip, WPAD, HTTP Injection, а также добавленный недавно SSH-MITM. К сожалению, из-за того что используемый способ маршрутизации трафика под Windows не дееспособен в линуксе, сложные MITM'ы в последнем (SSLStrip, SSL MITM, SMB hijack, LDAP relay, HTTP injection) не работают. Но все остальные — прекрасно. Про то, как использовать эти техники, лучше почитать в официальной вики проекта.



Intercepter-NG

Subterfuge

Ссылка на сайт

У пользователей Windows есть такой замечательный инструмент для проведения MITM-атак, как Intercepter-NG: куча различных техник, графический интерфейс. Правда, из-за различия в механизмах маршрутизации трафика между Windows и Linux некоторые MITM-техники в последнем не работают (SSLStrip, SSL MITM, SMB hijack, LDAP relay, HTTP injection). В связи с этим пользователям nix-систем приходится искать альтернативы. В большинстве случаев проведение сложной MITM выливается в использование сразу нескольких утилит (например, Ettercap, Arpspoof, SSLStrip), что достаточно неудобно. Именно поэтому и появился на свет проект Subterfuge, который, как это часто бывает, был представлен миру на хакерской конференции DEF CON 20. Установка предельно проста, сначала скачиваем с официального файла последнюю версию: `SubterfugePublicBeta5.0.tar.gz`**. Затем открываем терминал и выполняем**

```
tar -zxvf /root/Desktop/SubterfugePublicBeta5.0.tar.gz -C /root/Desktop
cd /root/Desktop/subterfuge
python install.py
```

После чего запустится гуишный установщик, который сделает процесс инсталляции максимально простым. Кстати, утилита имеет веб-интерфейс, поэтому сначала запускаем тулзу командой `subterfuge`**, а затем открываем браузер и вводим в адресной строке** `127.0.0.1`**. Можно сразу же нажать на** `Start` **и ждать, пока Subterfuge будет собирать пароли, которые летают по твоей локалке. Или же можно настроить точечную атаку на конкретный хост, для этого есть кнопка Settings. Еще несколько опций, достойных упоминания:**

- **Session Hijacking: крадет куки скомпрометированной сессии, для того чтобы атакующий мог аутентифицироваться в веб-сервисе;**

- HTTP code injection: позволяет внедрять различные пейлоады в скомпрометированную сессию;
- Evilgrade: позволяет использовать утилиту Evilgrade и подсовывать пользователям вместо файлов обновлений свои бинарники.



Subterfuge

Dsniff

Ссылка на сайт

Dsniff — это не одна утилита, а целый тулсет, который изначально был написан для аудита сетей и проведения пентестов, но, как и все подобные инструменты, может быть использован и в незаконных целях: для сбора логинов/паролей, прослушивания чужого трафика и так далее. В его состав входят следующие инструменты:

- arpspoof — понятно без комментариев, для чего нужен;
- dnsspoof — работает подобно arpspoof и позволяет подделывать DNS-ответы для DNS-сервера локальной сети;
- dsniff — представляет собой перехватчик паролей (password sniffer), который распознает несколько различных протоколов, включая Telnet, FTP, SMTP, POP (Post Office Protocol), IMAP (Internet Message Access Protocol), HTTP, CVS, Citrix, SMB (Server Message Block), Oracle и многие другие;
- filesnarf — позволяет собрать файл из захваченного tcpdump'ом NFS-трафика;
- macof — заполнит локальную сеть случайными воображаемыми MAC-адресами в надежде, что коммутатор перестанет срабатывать, как полагается, и начнет действовать подобно хабу, позволяя инструменту dsniff действовать более успешно в сетевом окружении коммутатора;
- sshmitm — утилита для перехвата SSH-трафика, правда, умеет работать только с первой версией протокола.

И это еще не все. Если интересно, про остальные можешь почитать на официальном сайте. К большому сожалению, проект уже давно не обновляется, но большинство техник и инструментов все равно остаются актуальными.

root@bt: ~ - Shell - Konsole <3>

Session Edit View Bookmarks Settings Help

```
dsniff: trigger_set_tcp: port 6003 -> x11
dsniff: trigger_set_tcp: port 6004 -> x11
dsniff: trigger_set_tcp: port 6005 -> x11
dsniff: trigger_set_tcp: port 6666 -> napster
dsniff: trigger_set_tcp: port 6667 -> irc
dsniff: trigger_set_tcp: port 6668 -> irc
dsniff: trigger_set_tcp: port 6669 -> irc
dsniff: trigger_set_tcp: port 7599 -> tds
dsniff: trigger_set_tcp: port 7777 -> napster
dsniff: trigger_set_tcp: port 8080 -> http
dsniff: trigger_set_tcp: port 8888 -> napster
dsniff: trigger_set_tcp: port 9898 -> aim
dsniff: trigger_set_tcp: port 65301 -> pcanywhere
dsniff: trigger_set_rpc: program 100005 -> mountd
dsniff: trigger_set_rpc: program 100004 -> ypserv
dsniff: trigger_set_rpc: program 100009 -> yppasswd
dsniff: listening on eth0
dsniff: trigger_tcp: decoding port 21 as ftp
-----------------
04/15/09 15:03:09 tcp 10.0.2.4.35059 -> pub2.kernel.org.21 (ftp)
USER anonymous
PASS me@me.com
```

Shell

Dsniff за работой

KARMA

Ссылка на сайт

Ну а теперь немного об инструментах, позволяющих пошалить в беспроводных сетях. Итак, KARMA — это набор утилит для оценки безопасности беспроводных клиентов, представляет собой беспроводной снифер, который, пассивно прослушивая 802.11 Probe Request фреймы, позволяет обнаруживать клиентов и их предпочтительные/доверенные сети. А затем проводит атаку Evil Twin, чтобы организовать MITM. То есть создается копия беспроводной точки доступа, находящейся в радиусе приема пользователя, тем самым оригинальная точка доступа подменяется двойником, к которому подключается пользователь, открывая злоумышленнику возможность доступа к конфиденциальной информации. Все дело в том, что большинство беспроводных устройств, в том числе ноутбуки, смартфоны, планшеты, автоматически подключаются к беспроводным AP, которые они запомнили. Не вдаваясь в подробности, когда ты включаешь свой ноут, сетевая карточка автоматически отсылает запросы, спрашивающие «Такая-то беспроводная сеть здесь?» Как ты понял, для того чтобы встроиться в середину, надо на такой запрос ответить положительно. Кстати говоря, этот принцип нашел применение в таком девайсе, как WiFi Pineapple Mark IV. Также KARMA используют еще несколько небезызвестных проектов: Pwnie Express, Kali Linux, Snoopy, Jasager.

AirJack

Ссылка на сайт

Одна из лучших, по мнению многих экспертов, утилит (а вернее, это сразу пакет утилит) для генерации и инъекции различных 802.11 фреймов. Изначально создавалась как инструмент разработчика — для захвата и внедрения пакетов в беспроводных сетях. Но, как обычно, в умелых руках AirJack превращается в мощное оружие, которое умеет инжектить фреймы прекращения сеанса (довольно

распространенная техника DoS- и MITM-атак), обнаруживать скрытые SSID и выполнять некоторые другие полезные функции.

SSLsplit

Ссылка на сайт

Ну а это проект, который активно используют многие из рассмотренных сегодня инструментов. SSLsplit — это тулза для проведения MITM-атак на SSL/TLS защищенные соединения. Соединения прозрачно перехватываются через механизм трансляции сетевых адресов и перенаправляются в SSLsplit, который завершает текущее соединение и инициирует новое уже от своего имени, логируя все передаваемые данные. Утилита поддерживает TCP-, SSL-, HTTP- и HTTPS-соединения в IPv4- и IPv6-сетях. Для SSL- и HTTPS-соединений SSLsplit на лету генерирует и подписывает поддельный сертификат X509v3. Кстати говоря, хороший мануал по тому, как с помощью SSLsplit прозрачно снифать SSL/TLS-соединения, включая протоколы, отличные от HTTP(S), можно посмотреть тут. Очень интересная утилита, настоятельно рекомендую установить и поиграть с ней самостоятельно.

```
root@kali:~/pemcrack-master# openssl rsa -in test.pem -out ca.key
Enter pass phrase for test.pem:
writing RSA key
root@kali:~/pemcrack-master# sslsplit -D -l connections.log -S /var/log/sslsplit
 -k ca.key -c ca.cer ssl 0.0.0.0 8443
Generated RSA key for leaf certs.
SSLsplit 0.4.10 (built 2015-03-02)
Copyright (c) 2009-2014, Daniel Roethlisberger <daniel@roe.ch>
http://www.roe.ch/SSLsplit
Build info: V:GIT
Features: -DHAVE_NETFILTER
NAT engines: netfilter* tproxy
netfilter: IP_TRANSPARENT SOL_IPV6 !IPV6_ORIGINAL_DST
Local process info support: no
compiled against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
rtlinked against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
TLS Server Name Indication (SNI) supported
OpenSSL is thread-safe with THREADID
Using SSL_MODE_RELEASE_BUFFERS
Using direct access workaround when loading certs
SSL/TLS protocol availability: ssl3 tls10 tls11 tls12
```

Пример использования утилиты SSLsplit

Superfish

В довольно интересную ситуацию попала компания Lenovo. Она предустанавливала на свои ноутбуки расширение Superfish, задачей которого было внедрять таргетированную рекламу в соответствие с пользовательскими интересами. Обнаружили такую фичу юзеры, не поленившиеся заглянуть в свойства SSL-сертификатов при установке защищенных соединений. Оказалось, что все сертификаты выданы некоей корпорацией Superfish Inc. Функции расширения Superfish заключались в следующем:

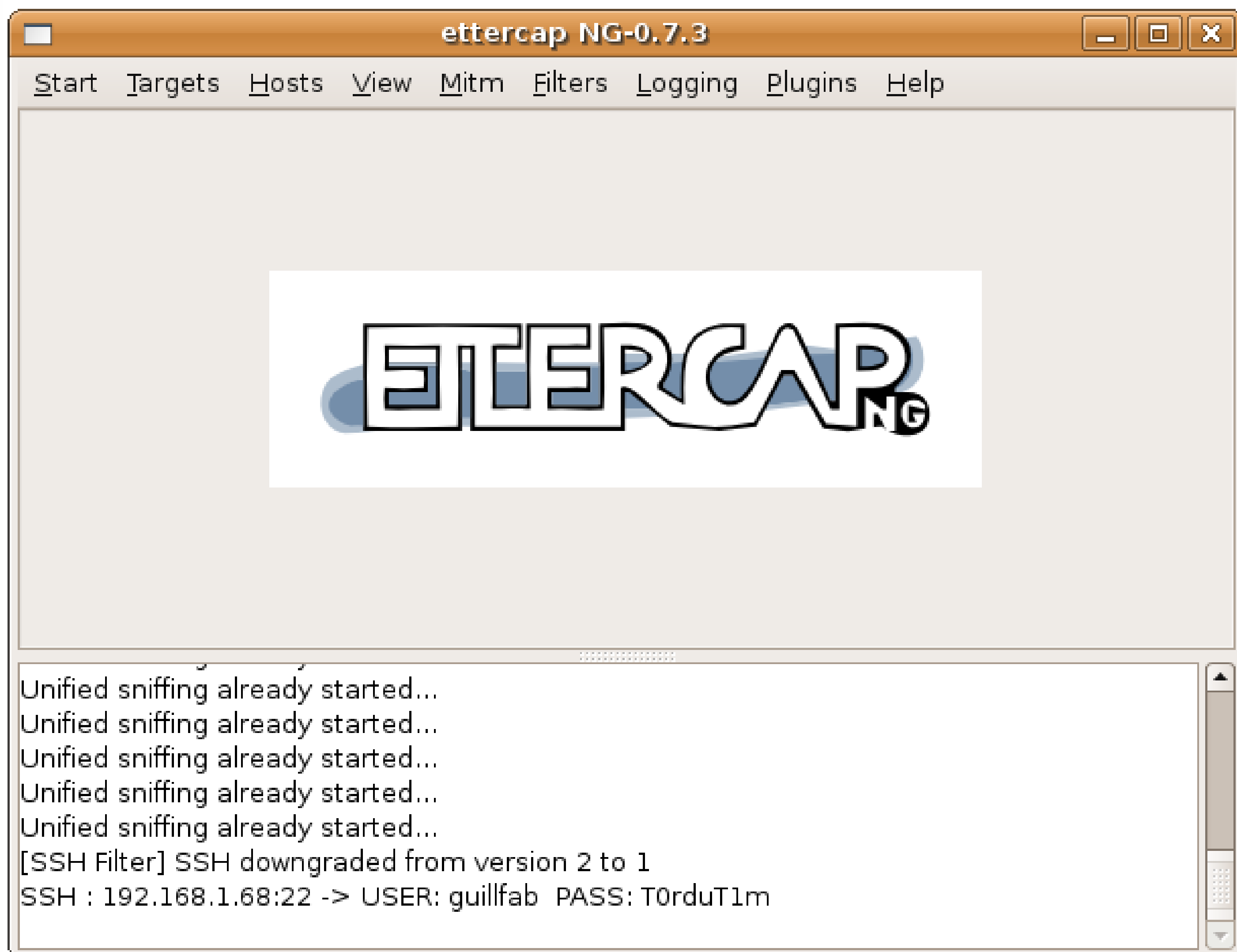
- взлом защищенных соединений с помощью атаки MITM;
- отображение собственного фальшивого сертификата (SHA-1, 1024-битный RSA) вместо настоящего;
- отслеживание действий пользователя;
- сбор персональной информации и загрузка ее на удаленный сервер;
- внедрение рекламы на посторонние веб-страницы;
- отображение всплывающих окон с рекламой.

Как видишь, даже крупные компании не брезгуют проведением MITM-атак. Обнадеживает лишь то, что компания публично покаялась в установке троянской программы на свои ноутбуки и дала обещание больше так не делать.

Ettercap

Ссылка на сайт

Ну а это утилита вообще одно из первых, что должно приходить на ум, как только услышишь «MITM-атака». Инструмент довольно старый, но продолжает активно обновляться, что не может не радовать. Подробно рассказывать про его возможности смысла нет, за четырнадцать лет существования он не раз освещался в журнале. А посему перелистай свою подшивку][, ну или же почитай в Сети руководства наподобие этого.



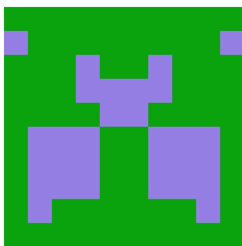
Внешний вид утилиты Ettercap

In The End

Как обычно, мы рассмотрели не все утилиты, а лишь наиболее популярные, есть еще немало малоизвестных проектов, о которых мы, возможно, как-нибудь поговорим. Как видишь, недостатка в инструментах для проведения MITM-атак не наблюдается, причем, что бывает не так уж часто, одна из крутых тулз реализована под винду. Про nix-системы и говорить нечего — целое разнообразие. Так что, думаю, ты всегда сможешь найти подходящий инструмент для угона чужих credentials. Упс, то есть для проведения аудита 🙂

Оцени статью:





Антон Жуков

Редактор рубрики «ВЗЛОМ»

Теги: MiTM Взлом Выбор редактора Статьи Таргетированные атаки